I CLAIM:

1. A method for authenticating a user, comprising the steps of:

(a) receiving a claimed identity of a user;

(b) receiving a first authentication sample from said user via a first communication channel;

(c) establishing a second communication channel with said user;

(i) said second communication channel being out-of-band with respect to said first communication channel;

(d) performing at least a portion of a challenge-response protocol, regarding a second authentication sample, with said user over said second communication channel;

(e) verifying at least one of said first and second authentication samples based on a stored template uniquely associated with said claimed identity;

(f) verifying another of said authentication samples in a manner independent of said verifying in (d); and

(g) granting access to said user based on said verifying in steps (e) and (f).

2. The method of claim 1, wherein said step (d) includes:

(1) prompting said user via said second communication channel to provide at least one of said authentication samples; and

(2) receiving said prompted authentication sample via said first communication channel.

3. The method of claim 1:

(1) wherein at least one of said authentication samples is spoken; and

(2) further comprising converting said spoken authentication sample into textual form via the application of speech recognition techniques.

4. The method of claim 1:

(1) wherein at least one of said authentication samples is spoken; and

(2) said (e) includes authenticating a unique vocal characteristic of said user by applying a speaker verification protocol involving (i) said claimed identity, (ii) said template, and (iii) said spoken authentication sample.

5. The method of claim 1 further comprising updating a template database based on at least one of said verified authentication samples.

6. The method of claim 1 where said first communication channel is telephonic and said second communication channel is a computer network.

7. The method of claim 1:

(1) where said first and said second authentication samples are provided in spoken form; and

(2) further comprising converting at least one of said spoken authentication samples to textual form for verification.

8. The method of claim 1 where at least one of said authentication samples is a biometric attribute.

9. The method of claim 1 where at least one of said authentication samples is a dynamically changing attribute held by said user.

10. The method of claim 1, wherein said step (a) includes the step of determining a telephonic caller identification of said user.

11. The method of claim 1, wherein said step (f) includes the steps of:

(1) generating a first string based on said another authentication sample;

(2) independently generating a second string based on said claimed identity;

(3) digitally comparing said first and second strings; and

(4) authenticating said another authentication sample if said strings match.

12. The method of claim 1 further comprising enabling a single sign-on process by sharing said authentication across multiple applications requiring authentication during a common session.

13. A method for authenticating a user, comprising the steps of:

(a) receiving a claimed identity of a user;

(b) receiving a first authentication sample from said user via a first communication channel;

(c) receiving a second authentication sample from said user via a second communication channel;

(d) verifying at least one of said first and second authentication samples based on a stored template uniquely associated with said claimed identity; and

(e) verifying another of said authentication samples in a manner independent of said verifying in (d); and

(f) granting access to said user based on said verifying in steps (d) and (e).

14. The method of claim 13:

(1) where said second communication channel is out-of-band with respect to said first communication channel; and

(2) further comprising, between said steps (a) and (c), prompting said user to use said second communication channel in response to determining that said first communication channel is insufficiently secure for the application environment.

15. A method for authenticating a user, comprising the steps of:

(a) obtaining a claimed identity of a user to be authenticated;

(b) prompting a user to speak a secure passcode via a communication channel;

(c) biometrically authenticating said user's voice by:

(i) obtaining a stored vocal characteristic unique to said claimed identity,

(ii) extracting a vocal characteristic of said user based on said spoken secure passcode, and

(iii) comparing said stored vocal characteristic and said extracted vocal characteristic;

(d) authenticating said secure passcode by:

(i) obtaining a regenerated passcode corresponding to said claimed identity, and

(ii) comparing said regenerated passcode and said spoken passcode; and

(e) granting access to said user if said user's voice and said passcode are authenticated based on steps (c) and (d).

16. A system for providing access to a secure application after user authentication, comprising:

(a) a portal subsystem configured to:

(i) receive a first user authentication sample via a first communication channel,

(ii) authenticate said first authentication sample via a biometric process;

(b) an authentication subsystem coupled to:

(i) said portal subsystem, and

(ii) a second communication channel which is out-of-band with respect to said first communication channel;

(c) said authentication subsystem being configured to:

(i) prompt a user via said portal subsystem to provide a sample over said second communication channel,

(ii) receive said second authentication sample via said second communication channel, and

(iii) authenticate said second authentication sample; and

(d) an application server:

(i) connected to said portal subsystem and said authentication subsystem, and

(ii) providing access to said user upon successful authentication of both said first and second authentication samples.

17. A system for providing user authentication to control access to a protected application, comprising:

(a) an interface, configured to receive a claimed identity of a user;

(b) an interface, connected to a first communication path, configured to receive a first authentication datum associated with said user;

(c) an interface, connected to a second communication path to said user which is out-of-band with respect to said first communication path;

(d) means for performing, over said second communication path, at least a portion of a challenge-response communication regarding a second authentication datum associated with said user;

(e) means for verifying said first authentication datum based on a nominal identity of said user; and

(f) means for verifying said second authentication datum independently of (e); and

(g) means for granting access to said user after both authentication data are verified.

18. The system of claim 17, where (d) further comprises means for prompting said user via said second communication path to provide said second authentication sample via said first communication path.

19. The system of claim 17 where said first communication path is telephonic and said second communication path is a computer network.

20. The system of claim 17:

(1) where both authentication data are received in oral form; and

(2) further comprising a speech-to-text module configured to convert at least one of said authentication data to textual form for verification.

21. A system for providing user authentication to control access to a protected application, comprising:

(a) means for prompting a user to speak a secure passcode to a system interface;

(b) a biometric authenticator configured to:

(i) extract a prosodic feature of said user based on said spoken secure passcode, and

(iii) verify said extracted prosodic feature against a stored prosodic template of said user;

(d) a passcode authenticator configured to:

(i) regenerate a passcode corresponding to said spoken passcode, and

(ii) verify said regenerated passcode against said spoken passcode; and

(e) means for granting access to said user after authenticating said user's voice and said passcode.

22. A computer-readable medium for authenticating a user, comprising logic instructions that, if executed:

(a) receive a claimed identity of a user;

(b) receive a first authentication sample from said user via a first communication path;

(c) establish a second communication path with said user;

(i) said second authentication path being out-of-band with respect to said first communication path;

(e) perform at least a portion of a challenge-response protocol, regarding a second authentication sample, with said user over said second communication path;

(e) verify at least one of said first and second authentication samples based on a stored template uniquely associated with said claimed identity; and

(f) verify another of said authentication samples in a manner independent of said verifying in (e); and

(g) grant access to said user based on said verification in (e) and (f).

23. The system of claim 22, wherein at least one of said means for receiving includes:

(1) means for prompting said user via said first communication channel to provide at least one of said authentication samples; and

(2) means for receiving said prompted authentication sample via said second communication channel.

24. The computer-readable medium of claim 22 where said first communication channel is telephonic, and said second communication channel is a computer network.

25. The computer-readable medium of claim 22:

(1) where said first and said second authentication samples are in spoken form; and

(2) further comprising logic instructions that, if executed, convert at least one of said spoken authentication samples to textual form for verification.

26. A computer-readable medium for authenticating a user, comprising logic instructions that, if executed:

(a) obtain a claimed identity of a user to be authenticated;

(b) prompt a user to speak a secure passcode via a communication channel;

(c) biometrically authenticate said user's voice by:

(i) obtaining a stored vocal characteristic unique to said claimed identity,

(ii) extracting a vocal characteristic of said user based on said spoken secure passcode, and

(iii) comparing said stored vocal characteristic and said extracted vocal characteristic;

(d) authenticate said secure passcode by:

(i) obtaining a regenerated passcode corresponding to said claimed identity, and

(ii) comparing said regenerated passcode and said spoken passcode; and

(e) grant access to said user if said user's voice and said passcode are authenticated based on (c) and (d).